State of Arizona
Government Information Technology Agency

Technology Security Assessment (TeSA) System
Guidelines For FY 2004

Background

The State's IT Planning Policy, P136, and Risk Management Standard, P800-S805, mandate that each executive branch agency shall submit an annual IT Security Assessment to GITA. The categories of controls addressed in the assessment derive from the Federal IT Security Framework and the Federal Office of Management and Budget's control requirements for agencies. In addition, Arizona's implementation plans for domains within the Enterprise Architecture (EA) call for gaps from target to be addressed as part of each agency's annual IT planning activities.

In the past, agencies have responded to questions about the security controls (management, operational, technical, and personnel) they employ using a Word document and returned the answers to GITA to be compiled.

GITA developed a new online assessment tool (TeSA) which provides increased security as well as ease of use and faster reporting of results. It maintains the Word document's relationships between categories of controls and individual control items but the questions from the Word document have been replaced by statements against which the agency measures its level of progress at implementing each particular security control.

Purpose

The purpose of the Information Technology Security Assessment is to help agencies identify their IT security vulnerabilities and then develop a plan to address them.

The completed assessment establishes a baseline for agency security operations. Subsequent annual assessments will then display progress as the agency identifies increases in the levels of effectiveness of various controls over time.

Requirements

Each executive branch agency must assess its IT environment, using the TeSA application, by September 1 of every year.

For 2004, 22 categories are assessed with several controls within each. There are five levels of effectiveness to be reported for each control. The five levels of effectiveness are as follows:

- Control Level One, Policy, requires an up-to-date, approved, Statewide or agency policy governing the item to be in place.
- Control Level Two, Procedure, requires an up-to-date, written, approved agency procedure to be in place and available to those who perform the activity.
- Control Level Three, Implemented, requires that work be carried out and managed in accordance with the documented procedures in Control Level Two.
- Control Level Four, Tested, requires the security control implemented in Level Three to be evaluated for adequacy and effectiveness and that, at a minimum, the control be updated whenever significant change occurs.
- Control Level Five, Integrated, requires that the security control implemented in Level Three be fully integrated within the organizational culture of the agency as part of an active, enterprise-wide program that has associated metrics.

For 2004, only the first three levels of effectiveness are required for a control to be considered "in place" at an agency. The TeSA online tool provides an accompanying Gap Plan field for each control statement having a level of effectiveness below "Implemented." This provides flexibility to the agencies in addressing individual gaps. However, GITA realizes the amount of effort this introduces to those agencies not requiring this level of detailed explanation. Where a lower level of detail is desired, an agency may simply describe the implementation plan in one of the control statements and refer to it from the others in that category.

The overall goal of the gap exercise is to have the agency plan a method of closing gaps in IT security, regardless of whether the gaps are reported for each security category or for each control.

Access, Help and Training

For access into the TeSA system, training, or for any other assistance, please call Jim Ryan at 602-364-4771 or e-mail jryan@gita.state.az.us.